What is claimed is:

1. A method for operating an access control system to camouflage a secret so as to be accessible by an authorized user yet protected against unauthorized access, said method comprising the steps of:

(a) representing in digital form a secret to be protected against unauthorized access;

(b) storing a plurality of computer-represented objects related to said secret;

(i) at least one of said objects being accessible by an authorized user as a password;

(ii) at least another of said objects being stored in a computer-readable wallet accessible to said access control system; and

(c) representing said secret as a function of said plurality of objects, using a composition function; and

(d) storing, in a computer-readable memory, said composition function:

(i) in a manner accessible to said access control system;

(ii) so as to be executable to generate a candidate secret using a user-inputted candidate password in conjunction with at least said another object stored in said wallet;

(iii) said generated candidate secret not regenerating said secret if said candidate password is not said password; and

(iv) said generated candidate secret regenerating said secret if said candidate password is said password;

thereby protecting said secret against unauthorized access by persons not having said password.

2. The method of claim 1 further comprising effecting a multilevel camouflaging scheme by camouflaging said at least another object stored in said wallet.

3. The method of claim 1 where:

(a) said secret represents linkage information among nodes of a network;

(b) said object accessible by an authorized user is a first graph representing at least a portion of said linkage information; and

(c) said object stored in said wallet is a second graph representing at least a portion of said linkage information; and

(d) said composition function accepts as operands at least said first and second graphs.

4. The method of claim 1 where:

(a) said secret represents at least one possible state of a system expressible as a Boolean logic function;

(b) said object accessible by an authorized user is a first matrix representing at least one of said states of said Boolean function;

(c) said object stored in said wallet is a second matrix representing at least one of said states of said Boolean function; and

(d) said composition function accepts as operands at least said first and second matrices.

5. The method of claim 1 where:

(i) said secret is a private key of said user;

(ii) said object accessible by said user is a PIN of said user;

(iii) said another object stored in said wallet is a pseudo-valid PIN; and

(iv) said candidate secret has the structural form of a private key.

6. A method for operating an access control system to release a secret camouflaged to be accessible to an authorized user yet protected against unauthorized access, said method comprising the steps of:

(a) accessing a plurality of computer-represented objects related to a secret;

(i) at least one of said objects being accessible by an authorized user as a password;

(ii) at least another of said objects being stored in a computer-readable wallet accessible to said access control system; and

(b) accessing a composition function representing said secret as a function of said plurality of objects;

(c) receiving a candidate password inputted by a user;

(d) generating a candidate secret for said user by executing said composition function using as operands thereto said candidate password in conjunction with at least said another object stored in said wallet;

(i) said generated candidate secret not regenerating said secret if said candidate password is not said password;

(ii) said generated candidate secret regenerating said secret if said candidate password is said password; and

(e) outputting said candidate secret to said user of said access control system.

7. The method of claim 6 where in said step (d)(i) said candidate secret is configured to deceive an unauthorized user into believing that said candidate secret is said secret.

8. The method of claim 6 where:

(a) said secret represents linkage information among nodes of a network;

(b) said object accessible by an authorized user is a first graph representing at least a portion of said linkage information;

(c) said object stored in said wallet is a second graph representing at least a portion of said linkage information; and

(d) said composition function accepts as operands at least said first and second graphs.

9. The method of claim 6 where:

(a) said secret represents at least one possible state of a system expressible as a Boolean logic function;

(b) said object accessible by an authorized user is a first array representing at least one of said states of said Boolean function; and

(c) said object stored in said wallet is a second array representing at least another of said states of said Boolean function; and

(d) said composition function accepts as operands at least said first and second arrays.

10. The method of claim 6 where:

(i) said secret is a private key of said user;

(ii) said object accessible by said user is a PIN of said user;

(iii) said another object stored in said wallet is a pseudo-valid PIN; and

(iv) said candidate secret has the structural form of a private key.

11. A method for operating an access control system to protect state information against unauthorized access, said method comprising the steps of:

(a) obtaining state information represented in digital form;

(b) deriving from said state information a first matrix;

(c) storing said first matrix as a password usable by an authorized user;

(d) deriving from said state information a second matrix;

(e) storing said second matrix in a computer-readable wallet accessible to said access control system; and

(f) storing, in a computer-readable memory, a composition function executable to generate a candidate matrix using a user-inputted candidate password in conjunction with said second matrix;

(i) said generated candidate state information not regenerating said matrix if said candidate password is not said password; and

(ii) said generated candidate state information regenerating said matrix if said candidate password is said password;

thereby protecting said state information against unauthorized access by persons not having said password.

12. The method of claim 11 further comprising effecting a multilevel access control scheme by camouflaging said second matrix.

13. The method of claim 11 where said state information includes a graph representing the status of a network characterized by nodes and links among at least some of said nodes.

14. The method of claim 13 used to protect an arbitrary secret representable in digital form, by representing said secret as interconnections among certain of said nodes, said interconnections being represented by values of said graph.

15. The method of claim 14 where said graph, if expressed as a matrix in row- or column-major order, would comprise an array having values representing said secret.

16. The method of claim 14 where said representing said secret includes padding said secret with sufficient bits to form a perfect square.

17. The method of claim 13 where said graph is an undirected graph.

18. The method of claim 13 where said graph is a directed graph.

19. The method of claim 11 where said state information comprises at least an array including a plurality of output values of a Boolean function, each output value corresponding to a unique sequence of input values for operands of said Boolean function.

20. The method of claim 19 where said state information further includes said sequences of input values corresponding to each of said output values.

21. The method of claim 19 where:

(a) said first and second matrices comprise arrays; and

(b) said state information array represents output values of a Boolean function, said output values being ordered in a manner corresponding to a known but unstored hierarchy of sequences of possible input values to said Boolean function.

22. The method of claim 19 used to protect an arbitrary secret expressed in digital form, by representing said secret as the values of said state information array.

23. The method of claim 22 where said representing said secret includes padding said secret with sufficient bits to form an integer power of a base used in the computational logic of the access control system.

24. A method for operating an access control system to protect state information against unauthorized access, said method comprising the steps of:

(a) retrieving a first matrix related to said state information from a computer-readable wallet accessible to said access control system;

(b) accessing a composition function representing said state information as a function of said first matrix and a password stored as a second matrix;

(c) receiving a candidate password inputted by a user;

(d) generating candidate state information for said user by executing said composition function using as operands thereto said candidate password in conjunction with at least said first matrix stored in said wallet;

(i) said generated candidate state information not regenerating said state information if said candidate password is not said password;

(ii) said generated candidate state information regenerating said state information if said candidate password is said password; and

(e) outputting said candidate state information to said user of said access control system.

25. The method of claim 24 where at least one of said matrices is an array represented using row- or column-major ordering.

26. The method of claim 24 where at least one of said matrices is stored on a smart card accessible to said user.

27. The method of claim 24 where said state information includes a graph representing the status of a network characterized by nodes and links among at least some of said nodes.

28. The method of claim 27 where said graph takes the form of an adjacency matrix.

29. The method of claim 27 where said composition function includes graph addition.

30. The method of claim 27 where said composition function includes a graph product operation.

31. The method of claim 27 used to protect an arbitrary secret representable in digital form, by representing said secret as interconnections among certain of said nodes, said interconnections being represented by values of said graph.

32. The method of claim 31 where said graph, if expressed as a matrix in row- or column-major order, would comprise an array having values equal to said secret.

33. The method of claim 27 where said network includes elements of a physical network.

34. The method of claim 27 where said network includes elements of a logical network.

35. The method of claim 24 where said state information comprises at least an array including a plurality of output values of a Boolean function, each output value corresponding to a unique sequence of input values for operands of said Boolean function.

36. The method of claim 35 where said state information further includes said sequences of input values corresponding to each of said output values.

37. The method of claim 35 where:

(a) said first and second matrices comprise arrays; and

(b) said state information array represents output values of a Boolean function, said output values being ordered in a manner corresponding to a known but unstored hierarchy of sequences of possible input values to said Boolean function.

38. The method of claim 37 used to protect an arbitrary secret expressed in digital form, by representing said secret as the values of said state information array.

39. A computer-readable medium containing logic instructions for operating an access control system to camouflage a secret so as to be accessible by an authorized user yet protected against unauthorized access, said logic instructions when executed:

(a) representing in digital form a secret to be protected against unauthorized access;

(b) storing a plurality of computer-represented objects related to said secret;

(i) at least one of said objects being accessible by an authorized user as a password;

(ii) at least another of said objects being stored in a computer-readable wallet accessible to said access control system; and

(c) representing said secret as a function of said plurality of objects, using a composition function; and

(d) storing, in a computer-readable memory, said composition function:

(i) in a manner accessible to said access control system;

(ii) so as to be executable to generate a candidate secret using a user-inputted candidate password in conjunction with at least said another object stored in said wallet;

(iii) said generated candidate secret not regenerating said secret if said candidate password is not said password; and

(iv) said generated candidate secret regenerating said secret if said candidate password is said password;

thereby protecting said secret against unauthorized access by persons not having said password.

40. The computer-readable medium of claim 39 where:

(a) said secret represents linkage information among nodes of a network;

(b) said object accessible by an authorized user is a first graph representing at least a portion of said linkage information; and

(c) said object stored in said wallet is a second graph representing at least a portion of said linkage information; and

(d) said composition function accepts as operands at least said first and second graphs.

41. The computer-readable medium of claim 39 where:

(a) said secret represents at least one possible state of a system expressible as a Boolean logic function;

(b) said object accessible by an authorized user is a first matrix representing at least one of said states of said Boolean function;

(c) said object stored in said wallet is a second matrix representing at least one of said states of said Boolean function; and

(d) said composition function accepts as operands at least said first and second matrices.

42. A computer-readable medium containing logic instructions for operating an access control system to release a secret camouflaged to be accessible to an authorized user yet protected against unauthorized access, said logic instructions when executed:

(a) accessing a plurality of computer-represented objects related to a secret;

  (i) at least one of said objects being accessible by an authorized user as a password;

  (ii) at least another of said objects being stored in a computer-readable wallet accessible to said access control system; and

(b) accessing a composition function representing said secret as a function of said plurality of objects;

(c) receiving a candidate password inputted by a user;

(d) generating a candidate secret for said user by executing said composition function using as operands thereto said candidate password in conjunction with at least said another object stored in said wallet;

(i) said generated candidate secret not regenerating said secret if said candidate password is not said password;

(ii) said generated candidate secret regenerating said secret if said candidate password is said password; and

(e) outputting said candidate secret to said user of said access control system.

43. The computer-readable medium of claim 42 where:

(a) said secret represents linkage information among nodes of a network;

(b) said object accessible by an authorized user is a first graph representing at least a portion of said linkage information;

(c) said object stored in said wallet is a second graph representing at least a portion of said linkage information; and

(d) said composition function accepts as operands at least said first and second graphs.

44. The computer-readable medium of claim 42 where:

(a) said secret represents at least one possible state of a system expressible as a Boolean logic function;

(b) said object accessible by an authorized user is a first array representing at least one of said states of said Boolean function; and

(c) said object stored in said wallet is a second array representing at least another of said states of said Boolean function; and

(d) said composition function accepts as operands at least said first and second arrays.

45. A computer-readable medium containing logic instructions for operating an access control system to protect state information against unauthorized access, said logic instructions when executed:

(a) obtaining state information represented in digital form;

(b) deriving from said state information a first matrix;

(c) storing said first matrix as a password usable by an authorized user;

(d) deriving from said state information a second matrix;

(e) storing said second matrix in a computer-readable wallet accessible to said access control system; and

(f) storing, in a computer-readable memory, a composition function executable to generate a candidate matrix using a user-inputted candidate password in conjunction with said second matrix;

(i) said generated candidate matrix not regenerating said state information if said candidate password is not said password; and

(ii) said generated candidate matrix regenerating said state information if said candidate password is said password;

thereby protecting said state information against unauthorized access by persons not having said password.

46. The computer-readable medium of claim 45 where said state information includes a graph representing the status of a network characterized by nodes and links among at least some of said nodes.

47. The computer-readable medium of claim 45 where said state information comprises at least an array including a plurality of output values of a Boolean function, each output value corresponding to a unique sequence of input values for operands of said Boolean function.

48. A computer-readable medium containing logic instructions for operating an access control system to protect state information against unauthorized access, said logic instructions when executed:

(a) retrieving a first matrix related to said state information from a computer-readable wallet accessible to said access control system;

(b) accessing a composition function representing said state information as a function of said first matrix and a password stored as a second matrix;

(c) receiving a candidate password inputted by a user;

(d) generating candidate state information for said user by executing said composition function using as operands thereto said candidate password in conjunction with at least said first matrix stored in said wallet;

  (i) said generated candidate state information not regenerating said state information if said candidate password is not said password;

  (ii) said generated candidate state information regenerating said state information if said candidate password is said password; and

(e) outputting said candidate state information to said user of said access control system.

49. The computer-readable medium of claim 48 where said state information includes a graph representing the status of a network characterized by nodes and links among at least some of said nodes.

50. The computer-readable medium of claim 48 where said state information comprises at least an array including a plurality of output values of a Boolean function, each output value corresponding to a unique sequence of input values for operands of said Boolean function.

51. An access control server configured to camouflage a secret so as to be accessible by an authorized user yet protected against unauthorized access, comprising:

(a) a computer processor;

(b) an interface configured to receive in digital form a secret to be protected against unauthorized access;

(c) a memory configured to store a plurality of computer-represented objects related to said secret;

(i) at least one of said objects being accessible by an authorized user as a password;

(ii) at least another of said objects being stored in a computer-readable wallet accessible to said access control system; and

(d) a memory configured to store a composition function representing said secret as a function of said plurality of objects:

(i) in a manner accessible to said access control system;

(ii) so as to be executable by said processor to generate a candidate secret using a user-inputted candidate password in conjunction with at least said another object stored in said wallet;

(iii) said generated candidate secret not regenerating said secret if said candidate password is not said password; and

(iv) said generated candidate secret regenerating said secret if said candidate password is said password;

thereby protecting said secret against unauthorized access by persons not having said password.

52. An access control server to release a secret camouflaged to be accessible to an authorized user yet protected against unauthorized access, comprising:

(a) a memory configured to store a plurality of computer-represented objects related to a secret;

(i) at least one of said objects being accessible by an authorized user as a password;

(ii) at least another of said objects being stored in a computer-readable wallet accessible to said access control server; and

(b) a memory configured to store a composition function representing said secret as a function of said plurality of objects;

(c) an interface configured to receive a candidate password inputted by a user;

(d) a computer processor configured to execute said composition function to generate a candidate secret for said user by using as operands thereto said candidate password in conjunction with at least said another object stored in said wallet;

(i) said generated candidate secret not regenerating said secret if said candidate password is not said password;

(ii) said generated candidate secret regenerating said secret if said candidate password is said password; and

(e) an interface configured to output said candidate secret to said user of said access control server.

53. An access control server to protect state information against unauthorized access, comprising:

(a) a computer processor;

(b) an interface configured to obtain state information represented in digital form;

(c) a decomposition module configured to decompose said state information into at least a first matrix and a second matrix;

(d) a memory configured to store said first matrix as a password usable by an authorized user;

(e) a memory configured to store said second matrix in a computer-readable wallet accessible to said access control server; and

(f) a memory configured to store a composition function executable by said processor to generate a candidate matrix using a user-inputted candidate password in conjunction with said second matrix;

(i) said generated candidate matrix not regenerating said state information if said candidate password is not said password; and

(ii) said generated candidate matrix regenerating said state information if said candidate password is said password;

thereby protecting said state information against unauthorized access by persons not having said password.

54. An access control server to protect state information against unauthorized access, comprising:

(a) a computer-readable wallet configured to store a first matrix related to said state information accessible to said access control server;

(b) a memory configured to store a composition function representing said state information as a function of said first matrix and a password stored as a second matrix;

(c) an interface configured to receive a candidate password inputted by a user;

(d) a computer processor configured to execute said composition function to generate candidate state information for said user by using as operands to said composition function said candidate password in conjunction with at least said first matrix stored in said wallet;

(i) said generated candidate state information not regenerating said state information if said candidate password is not said password;

(ii) said generated candidate state information regenerating said state information if said candidate password is said password; and

(e) an interface configured to output said candidate state information to said user of said access control server.

55. An access control system to camouflage a secret so as to be accessible by an authorized user yet protected against unauthorized access, comprising:

(a) means for representing in digital form a secret to be protected against unauthorized access;

(b) means for storing a plurality of computer-represented objects related to said secret;

(i) at least one of said objects being accessible by an authorized user as a password;

(ii) at least another of said objects being stored in a computer-readable wallet accessible to said access control system; and

(c) means for representing said secret as a function of said plurality of objects, using a composition function; and

(d) means for storing, in a computer-readable memory, said composition function:

(i) in a manner accessible to said access control system;

(ii) so as to be executable to generate a candidate secret using a user-inputted candidate password in conjunction with at least said another object stored in said wallet;

(iii) said generated candidate secret not regenerating said secret if said candidate password is not said password; and

(iv) said generated candidate secret regenerating said secret if said candidate password is said password;

thereby protecting said secret against unauthorized access by persons not having said password.

56. An access control system releasing a secret camouflaged to be accessible to an authorized user yet protecting against unauthorized access, said method comprising the steps of:

(a) means for accessing a plurality of computer-represented objects related to a secret;

(i) at least one of said objects being accessible by an authorized user as a password;

(ii) at least another of said objects being stored in a computer-readable wallet accessible to said access control system; and

(c) means for accessing a composition function representing said secret as a function of said objects;

(d) means for receiving a candidate password inputted by a user;

(e) means for generating a candidate secret for said user by executing said composition function using as operands thereto said candidate password in conjunction with at least said another object stored in said wallet;

(i) said generated candidate secret not regenerating said secret if said candidate password is not said password;

(ii) said generated candidate secret regenerating said secret if said candidate password is said password; and

(f) means for outputting said candidate secret to said user of said access control system.

57. An access control system to protect state information against unauthorized access, comprising:

(a) means for obtaining state information represented in digital form;

(b) means for deriving from said state information a first matrix;

(c) means for storing said first matrix as a password usable by an authorized user;

(d) means for deriving from said state information a second matrix;

(e) means for storing said second matrix in a computer-readable wallet accessible to said access control system; and

(f) means for storing, in a computer-readable memory, a composition function executable to generate a candidate matrix using a user-inputted candidate password in conjunction with said second matrix;

(i) said generated candidate matrix not regenerating said state information if said candidate password is not said password; and

(ii) said generated candidate matrix regenerating said state information if said candidate password is said password;

thereby protecting said state information against unauthorized access by persons not having said password.

58. An access control system to protect state information against unauthorized access, comprising:

(a) means for retrieving a first matrix related to said state information from a computer-readable wallet accessible to said access control system;

(b) means for accessing a composition function representing said state information as a function of said first matrix and a password stored as a second matrix;

(c) means for receiving a candidate password inputted by a user;

(d) means for generating candidate state information for said user by executing said composition function using as operands thereto said candidate password in conjunction with at least said first matrix stored in said wallet;

(i) said generated candidate state information not regenerating said state information if said candidate password is not said password;

(ii) said generated candidate state information regenerating said state information if said candidate password is said password; and

(e) means for outputting said candidate state information to said user of said access control system.

59. A method for operating an access control system to protect a secret against unauthorized access, said method comprising the steps of:

(a) obtaining a secret in digital form;

(b) modeling said secret as a graph;

(c) camouflaging said secret by decomposing said graph into:

(i) a first sub-graph to be distributed as a password to an authorized user of said system; and

(ii) a second sub-graph to be stored in a manner accessible to said system;

(iii) by relating said first and second sub-graphs to said graph via a composition function configured to regenerate said secret using a user-inputted candidate password in conjunction with said second sub-graph only when said candidate password is said password; and

(d) storing said camouflaged secret for subsequent access by a user;

thereby protecting said secret against unauthorized access by persons not having said password.

60. A method for operating an access control system to protect a secret against unauthorized access, said method comprising the steps of:

(a) obtaining a secret in digital form;

(b) modeling said secret as a matrix representing at least a portion of a truth table corresponding to a Boolean function;

(c) camouflaging said secret by decomposing said matrix into:

(i) a first portion to be distributed as a password to an authorized user of said system; and

(ii) a second portion to be stored in a manner accessible to said system;

(iii) by relating said first and second portions to said matrix via a composition function configured to regenerate said secret using a user-inputted candidate password in conjunction with said second portion only when said candidate password is said password; and

(d) storing said camouflaged secret for subsequent access by a user;

thereby protecting said secret against unauthorized access by persons not having said password.

61. A method for operating an access control system to protect a secret against unauthorized access, said method comprising the steps of:

(a) retrieving, from a computer-readable wallet, a first sub-graph:

(i) related to a secret camouflaged as a graph by said system; and

(ii) accessible to an authorized user as a password;

(b) accessing a composition function representing said secret as a function of said first sub-graph and a stored second sub-graph accessible to said system;

(c) receiving a candidate password inputted by a user;

(d) generating a candidate secret for said user by executing said composition function using as operands thereto said candidate password in conjunction with at least said first sub-graph;

(i) said generated candidate secret not regenerating said secret if said candidate password is not said password;

(ii) said generated candidate secret regenerating said secret if said candidate password is said password; and

(e) outputting said candidate secret to said user of said access control system.

62. A method for operating an access control system to protect a secret against unauthorized access, said method comprising the steps of:

(a) retrieving, from a computer-readable wallet, a first matrix:

(i) related to a secret camouflaged as a Boolean function by said system; and

(ii) accessible to an authorized user as a password;

(b) accessing a composition function representing said secret as a function of said first matrix and a stored second matrix accessible to said system;

(c) receiving a candidate password inputted by a user;

(d) generating a candidate secret for said user by executing said composition function using as operands thereto said candidate password in conjunction with at least said first matrix;

(i) said generated candidate secret not regenerating said secret if said candidate password is not said password;

(ii) said generated candidate secret regenerating said secret if said candidate password is said password; and

(e) outputting said candidate secret to said user of said access control system.

63. A computer-readable medium containing logic instructions for operating an access control system to protect a secret against unauthorized access, said logic instructions when executed:

(a) obtaining a secret in digital form;

(b) modeling said secret as a graph;

(c) camouflaging said secret by decomposing said graph into:

(i) a first sub-graph to be distributed as a password to an authorized user of said system; and

(ii) a second sub-graph to be stored in a manner accessible to said system;

(iii) by relating said first and second sub-graphs to said graph via a composition function configured to regenerate said secret using a user-inputted candidate password in conjunction with said second sub-graph only when said candidate password is said password; and

(d) storing said camouflaged secret for subsequent access by a user;

thereby protecting said secret against unauthorized access by persons not having said password.

64. A computer-readable medium containing logic instructions for operating an access control system to protect a secret against unauthorized access, said logic instructions when executed:

(a) obtaining a secret in digital form;

(b) modeling said secret as a matrix representing at least a portion of a truth table corresponding to a Boolean function;

(c) camouflaging said secret by decomposing said matrix into:

  (i) a first portion to be distributed as a password to an authorized user of said system; and

  (ii) a second portion to be stored in a manner accessible to said system;

  (iii) by relating said first and second portions to said matrix via a composition function configured to regenerate said secret using a user-inputted candidate password in conjunction with said second portion only when said candidate password is said password; and

(d) storing said camouflaged secret for subsequent access by a user;

thereby protecting said secret against unauthorized access by persons not having said password.

65. A computer-readable medium containing logic instructions for operating an access control system to protect a secret against unauthorized access, said logic instructions when executed:

(a) retrieving, from a computer-readable wallet, a first sub-graph:

  (i) related to a secret camouflaged as a graph by said system; and

  (ii) accessible to an authorized user as a password;

(b) accessing a composition function representing said secret as a function of said first sub-graph and a stored second sub-graph accessible to said system;

(c) receiving a candidate password inputted by a user;

(d) generating a candidate secret for said user by executing said composition function using as operands thereto said candidate password in conjunction with at least said first sub-graph;

(i) said generated candidate secret not regenerating said secret if said candidate password is not said password;

(ii) said generated candidate secret regenerating said secret if said candidate password is said password; and

(e) outputting said candidate secret to said user of said access control system.

66. A computer-readable medium containing logic instructions for operating an access control system to protect a secret against unauthorized access, said logic instructions when executed:

(a) retrieving, from a computer-readable wallet, a first matrix:

(i) related to a secret camouflaged as a Boolean function by said system; and

(ii) accessible to an authorized user as a password;

(b) accessing a composition function representing said secret as a function of said first matrix and a stored second matrix accessible to said system;

(c) receiving a candidate password inputted by a user;

(d) generating a candidate secret for said user by executing said composition function using as operands thereto said candidate password in conjunction with at least said first matrix;

(i) said generated candidate secret not regenerating said secret if said candidate password is not said password;

(ii) said generated candidate secret regenerating said secret if said candidate password is said password; and

(e) outputting said candidate secret to said user of said access control system.